UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/549,944	04/14/2000	Mohammad Peyravian	RSW9-2000-0038-US1	9149

25259 7590 03/19/2004

IBM CORPORATION
3039 CORNWALLIS RD.
DEPT. T81 / B503, PO BOX 12195
REASEARCH TRIANGLE PARK, NC 27709

EXAMINER	
ZAND, KAMBIZ	
ART UNIT	**PAPER NUMBER**
2132	

DATE MAILED: 03/19/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/549,944	PEYRAVIAN ET AL.	
	Examiner	Art Unit	
	Kambiz Zand	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 April 2000*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-12* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *6 and 10-12* is/are allowed.

6)☒ Claim(s) *1-5 and 7-9* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *14 April 2000* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date 2.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. **Claims 1-12** have been examined.

Drawings

2. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they include the following reference sign(s) not mentioned in the description: items "209 and 211" in fig.2. A proposed drawing correction, corrected drawings, or amendment to the specification to add the reference sign(s) in the description, are required in reply to the Office action to avoid abandonment of the application. The objection to the drawings will not be held in abeyance.

Information Disclosure Statement PTO-1449

3. The pages of the all references submitted by applicant have been considered.

Claim Objections

4. Claims 6, 9 and 10 are objected to because of the following informalities: Examiner considers phrases "si" and "-or'ing" in line 11 and 16 of the claim 6; phrase "programming" in line 22 of claim 9 and phrase "-or'ing" in line 19 of claim 10 as typo error. Examiner considers Phrases "is"; "programming" and "-oring" as corrected phrase. Appropriate correction is required.

5. Claim 1 recites the limitation "the server" in line 14 of the claim as a typo error. Examiner considers "the host computer" as the correct phrase. Appropriate correction is required.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. **Claims 1,5 and 7-9** are rejected under 35 U.S.C. 103(a) as being unpatentable over Davis et al (6,064,736 A) in view of Bird et al (5,148,479A).

As per claims 1, 5, 7 and 9 Davis et al (6,064,736 A) teach a computer network, a method and a computer program product (see fig.1 where a computer is connected to a local area network; col.3, lines 26-33) comprising: a local computer (see fig.1; col.3, lines 28-39), a userid associated with a user of the local computer (see fig.2, item 207 user id; col.3, lines 41-43 where a user id is associated with a client computer of the user), said userid having a secret password associated therewith (see fig.3 where the userid is associated with a password, item 309 and 307; col.4, lines 42-46); a host computer (see col.4, lines 45-46 where the server is the host computer; col.3, lines 41-

55; fig. 2 and 3 where the items 204 and 304 are the host computer respectively), a communications mechanism connecting the host computer to the local computer (see fig.1; fig.2-3 where the communication between the client and the server is being shown) wherein the local computer, requests access to the host computer by: sending the userid and a first nonce to the host computer (see fig.2, item 207 where the userid and the first nonce are transmitted from the client to the server or the host computer); the host computer responds to the local computer by sending a second nonce to the local computer (see fig.2, item 217 where the host computer or the server send second nonce called server nonce to the client or local computer), the local computer then sends the host Computer an authentication token comprising a hashed value of the combination of password and a nonce (see fig.5, item 531 where the salt value is the random value of a nonce and password that is being hashed and item 333 where by comparison the authentication is being done) **but do not disclose** the userid and password, the first nonce and the second nonce, a server verifies the hashed value using copies of the authentication token, first nonce and second nonce residing at the host computer; the host computer allows the user at the local computer to access information at the host computer only if the verification is successful. However Bird et al (5,148,479A) disclose the userid and password, the first nonce and the second nonce, a server verifies the hashed value using copies of the authentication token, first nonce and second nonce residing at the host computer; the host computer allows the user at the local computer to access information at the host computer only if the verification is successful (see fig.2 where N1 and N2 represent first and second nonce and where s

represent a shared secret such as a password between two parties and X also may be considered as a userid. Also consider that even without X the hashing of the first nonce and second nonce and the shared secret has been shown in fig.2 and their authentication procedure as disclosed in col.4-13 and where upon authentication access is granted). It would have been obvious to one of ordinary skilled in the art at the time the invention was made to utilize Bird's hashing of the second nonce + userid in Davis's hashing of the password and the first nonce in order to provide an improved two-party authentication system, methods and computer program products that can detect an intruder gaining access to password on a host computer.

As per claim 8 Davis et al (6,064,736 A) teach a network, a method and a computer program product as claimed in claim 2, 5 or 6 and 10 or 11 wherein said hash function is a collision resistant, one-way hash (see col.5, lines 5-8 where MD5 is a collision-resistant one way hash function).

Claim Rejections - 35 USC § 102

8. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

9. **Claims 2-4** are rejected under 35 U.S.C. 102(e) as being anticipated by Davis et al (6,064,736 A).

As per claim 2 Davis et al (6,064,736 A) teach a computer network comprising: a local computer (see fig.1; col.3, lines 28-39); a userid associated with a user of the local computer (see fig.2, item 207 user id; col.3, lines 41-43 where a user id is associated with a client computer of the user); said users having an original password associated therewith (see fig.3 where the userid is associated with a password, item 309 and 307; col.4, lines 42-46); a host computer (see col.4, lines 45-46 where the server is the host computer; col.3, lines 41-55; fig. 2 and 3 where the items 204 and 304 are the host computer respectively); and, a communications mechanism connecting the host computer to the local computer (see fig.1; fig.2-3 where the communication between the client and the server is being shown) wherein the local computer accesses the host computer by using the original password (see col.2, lines 15-18 where the client attempt for connection is validated by authenticating the password by the host computer or

server computer) and wherein the local computer changes the original password for accessing the host computer to a new password by sending a first random value and the userid of the user to the host computer (see col.5, lines 31-45 where the new password is created by using a newly random value, salt value at 612 of fig.6; and fig.6), the host computer generates a second random value and sends it to the local computer (see fig.5, item 519 and 521 from the server or host to client or local computer), the local computer generates an authentication token using a hash function (see fig.3), the users the original password and a digest of the new password and sends the authentication token and the digest to the host computer, wherein the host computer accepts the change of the password to the new password if the host computer can verify the authentication token (see col.5, lines 32-45 where upon authentication a new password is set).

As per claim 3 Davis et al (6,064,736 A) teach a network as claimed in claim 2 wherein the host computer verifies the authentication token using a copy of the first random value, a copy of the second random value and a copy of the authentication token residing at the host computer (see col.5, lines 17-67 and col.6, lines 1-23).

As per claim 4 Davis et al (6,064,736 A) teach a network, a method and a computer program product as claimed in claim 2, 5 or 6 and 10 or 11 wherein said hash function is a collision resistant, one-way hash (see col.5, lines 5-8 where MD5 is a collision-resistant one way hash function).

Allowable Subject Matter

Claims 6 and 10-12 are allowed.

The prior art of records singly or in combination do not teach the specific steps of Applicant's invention method and system and computer program product where securely changing an existing password associated with a user identifier users on a host computer to a new password, wherein said passwords enable a user associated with said users at a local computer to access information on said host computer across a network, said method comprising the steps of: computer readable programming means for sending, by the local computer, the users and a first nonce to the host computer; computer readable programming means for replying, by the host computer to the local computer, with a second nonce; computer readable programming means for generating, by the local computer, a first digest of the users and the existing password and a second digest of the users and the new password; computer readable programming means for creating, by the local computer, an authentication token and an authentication token mask wherein said authentication token is a hash function of the first digest, first nonce and second nonce, and said token mask is a hash function of the second digest, first nonce plus a predetermined value and the second nonce, computer readable programming means for generating, by the local computer, a protected digest by exclusive-or'ing the second digest with the token mask; computer readable programming means for sending, by the local computer to the host computer, the users

authentication token and the protected digest; computer readable programming means for verifying, by the host computer, the validity of the authentication token; and, computer readable programming means for accepting the new password to replace the existing password if the authentication token is valid.

Dependent claims 11-12 as being dependent upon Independent claim 10 and having additional allowable features therein.

Conclusion

10. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

U.S.Patent No. US (6,687,836 B1) teach method and apparatus which enable a computer user to verify whether they have correctly input their password into a computer.

U.S.Patent No. US (6,668,323 B1) teach method and apparatus for password protection of a data processing system that permit a user-selected password to be recovered.

U.S.Patent No. US (6,601,175 B1) teach method and system for providing limited-life machine-specific password for data processing systems.

U.S.Patent No. US (6,628,786 B1) teach distributed state random number generator and method for utilizing same.

U.S.Patent No. US (6,178,508 B1) teach system for controlling access to encrypted data files by a plurality of users.

U.S.Patent No. US (5,666,415 A) teach method and apparatus for cryptographic authentication.

U.S.Patent No. US (5,787,169 A) teach method and apparatus for controlling access to encrypted data files in a computer system.

U.S.Patent No. US (5,204,966 A) teach system for controlling access to a secure system.

U.S.Patent No. US (4,649,233) teach method for establishing user authentication with composite session keys among cryptographically communicating nodes.

11. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kambiz Zand whose telephone number is (703) 306-4169. The examiner can normally reached on Monday-Thursday (8:00-5:00). If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (703) 305-1830. The fax phone numbers for the organization where this application or proceeding is assigned as (703) 872-9306. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see

http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Kambiz Zand

03/15/04

GILBERTO BARRON
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100